Resource Scheduling under randomized scheduling algorithm (ROSA) in the Cloud Computing

[1]Jagruti Soni, [2]Prof. Prashant Jawalkar
[12]Department of Computer Engineering, Bhivarabai Sawant Institute of Technology & Research, Pune, India.

Abstract : Recently, there has been a dramatic increase in the popularity of cloud computing systems that rent computing resources on-demand, bill on a pay-as-you-go basis, and multiplex many users on the same physical infrastructure. It is a virtual pool of resources which are provided to users via Internet. It gives users virtually unlimited pay-per-use computing resources without the burden of managing the underlying infrastructure. One of the goals is to use the resources efficiently and gain maximum profit. Scheduling is a critical problem in Cloud computing, because a cloud provider has to serve many users in Cloud computing system. So scheduling is the major issue in establishing Cloud computing systems. The scheduling algorithms should order the jobs in a way where balance between improving the performance and quality of service and at the same time maintaining the efficiency and fairness among the jobs.

Keywords:- Encryption Algorithm, Data Privacy, Data Security, Notification System for Alert generation.

I. INTRODUCTION

Now a day's cloud computing is an intelligently developed technology to store data from number of client. Cloud computing allows users to remotely store their data over cloud. Remote backup system is the progressive technique which minimizes the cost of implementing more memory in an organization. It helps government agencies and enterprises to reduce financial overhead of data management. They can extract their data backups remotely to third party cloud storage providers than maintaining their own data centres. An individual or an organization does not require purchasing the storage devices. Instead they can store their data to the cloud and archive data to avoid information loss in case of system failure like hardware or software failures.

Cloud storage is more flexible, but security and privacy are available for the outsourced data becomes a serious concern. To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must after encryption of the file, store to the cloud. If a third person downloads the file, they can view the record if they had the key which is used to decrypt the encrypted file. To overcome the problem Cloud computing is one of the emerging technologies, which contains huge open distributed system. It is important to protect the data and privacy of user.

Attribute-based Encryption is one of the most suitable schemes for data access control in public clouds for it can ensures data owners direct control over data and provide a fine -grained access control service. Till now, there are many ABE schemes proposed, which can be divided into two categories; Key Policy Attribute -based Encryption (KP-ABE) as well as Ciphertext Policy Attribute-based Encryption (CPABE). In KP-ABE schemes, decrypt keys are combined with access structures and in ciphertexts it is labeled with special attribute sets, for attribute management and key distribution an authority is responsible. The authority may be the human resource department in a company, the registration office in a university, etc. The data owner defines the access policies and encrypts the data according to the defined policies. Every user will be issued a secret key reflecting its attributes. A user can decrypt the data whenever its attributes match the access policies.

Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or restricts access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much important for protection in computer security. The Cloud storage is a very important service in cloud computing. The Cloud Storage offers services for data owners to host their data over cloud environment. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not completely trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. Therefore the decentralized data access control scheme is introduced.

Cloud computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and enable users to enjoy ubiquitous, convenient and on demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead. Attracted by these appealing features, both individuals and enterprises are motivated to outsource their data to the cloud, instead of purchasing software and hardware to manage the data themselves. Despite of the various advantages of cloud services, outsourcing sensitive information (such as e-mails, personal health records, company finance data, government documents, etc.) to remote servers brings privacy concerns. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A general approach to protect the data confidentiality is to encrypt the data before outsourcing. However, this will cause a huge cost in terms of data usability.

Data security is one of the major worries in the adoption of cloud computing. Compared to conventional systems, users will lose their direct control over their data. In this paper, we will explore the problem of integrity verification for big data storage in cloud. This problem can also be called data auditing when the verification is conducted by a trusted third party(TP). From cloud user's viewpoint, it may also be called 'auditing-as-a-service'. our system supports updates with a size that is not restricted by the size of file blocks, thereby offers extra flexibility and scalability compared to existing schemes.

For better security, our system combines an additional authorization process with the aim of eliminating threats of unauthorized audit challenges from malicious or pretended third-party auditors, which we term as 'authorized auditing.

II. LITERATURE SURVEY

Hongwei In this paper Mashayekhy [1], demonstrates that Cloud providers provision their resources such as CPUs, memory, and storage by creating virtual machine (VM) instances which are then allocated to the users. The users are charged based on a pay-as you-go model, and their payment is determined by considering both incentives and the incentives of the cloud providers. Auction markets capture such incentives, where users name their own prices for their requested VMs. Here author design an auction based online mechanism for VM provisioning, allocation, and pricing in clouds that considers several types of resources. This proposed mechanism makes no assumptions about future demand of VMs, which is the case in real cloud environment. The proposed online mechanism is invoked as soon as a user places a request or some of the allocated resources are being released and then become available. The mechanism allocates VM instances to selected users for the period they requests, and then ensures that the users will continue using their VM instances for the entire requested period. Here mechanism determines the payment the users have to pay for using the allocated resources.

In this paper Himani [2], demonstrates that Scheduling is one of the most complicated task in cloud, which aims in scheduling the tasks most effectively which would help in reducing the turnaround time as well as improve performance. Since there are various objectives, the main role is to design, develop a best efficient scheduling technique to do proper separation of tasks on virtual machines. For this, author have used cost deadline based task scheduling algorithm by which it is being proven that approach is more efficient in the these parameters in Task Profit, Task Penalty, Throughput, Provider profit and User loss.

In this paper Aazam [3], the author deals with interoperability of multiple clouds, which can be also called as cloud federation or inter-cloud computing. In the cloud federation, services would be provided via two or more clouds. Once configured, inter-cloud computing can provide services which would be more scalable, better manageable, and most efficient. Those tasks are provided through a middleware entity called cloud broker. A broker is responsible for reserving resources, managing them, discovering services according to customer demands, Service Level Agreement (SLA) negotiation, and matchmaking between the involved service provider and the customer. Here the author has deployed a Holistic Brokerage model in which brokers are managing the users request and server resource utilization simultaneously. This paper concludes that, It would provide a efficient on-demand and advance service reservation, pricing for the cloud users.

In this paper Abbadi [4], author demonstrates about Managing allocation of cloud virtual machines. Current implementations of cloud schedulers do not entirely consider the cloud infrastructure neither do they consider the overall user and infrastructure properties. This results in major security, privacy, and resilience concerns. Author has introduced a Novel cloud scheduler which considers both user requirements and infrastructure properties is proposed. Open Stack is used as a Cloud environment where cloud scheduler is deployed. Comparing the performance metrics, This helps in providing trustworthiness among end users.

In this paper Feng [5], the author demonstrates that, there are increasing count of infrastructureas-aservice (IaaS) cloud providers who have started to provide cloud computing services, they have form a competitive market to compete for users of these services. Due to different resource capacities and various service workloads, users would observe different finishing times for their cloud computing tasks and experience different levels of service qualities as a result. To compete for cloud users, it is critically very much important for each cloud service provider to select an optimal price for their customers which would be most effective in terms of reliability of service. So here, Game Theory concept satisfying Nash Equilibrium is introduced. It provides Iaas cloud provider to select an optimal prices to compete with the other CSP.

III. PROPOSED SYSTEM

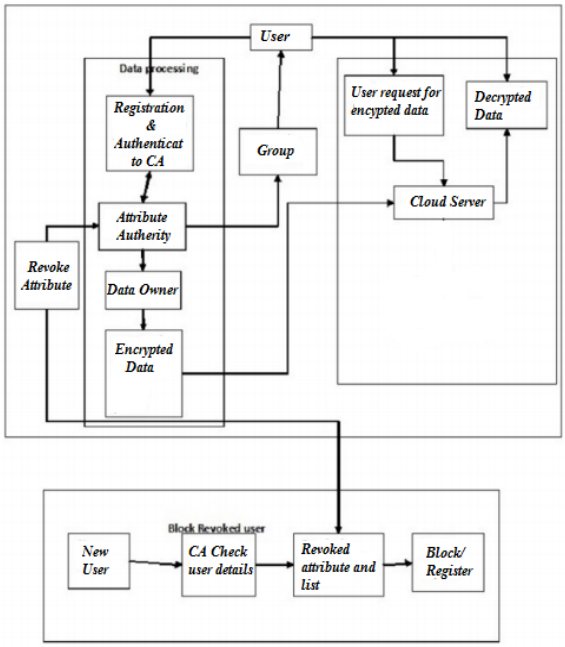

Fig 1. System architecture

User
This module helps clients to enter their query keyword to get the most important documents from set of uploaded documents. This module recovers the documents from cloud which coordinates the query keyword.

Data Owner
After expansion of keywords the data owner assist data with encrypting the document utilizing encryption Algorithm and after that upload the encrypted document to the cloud for storage reason. This permits data owner to store their secret key in extremely secure way without presenting it to the clients of framework. For this, secret key is put away again in encrypted frame.

Download Ranked Results
Clients/user can download the resultant arrangement of documents just if he/she is approved client who has allowed consent from data owner to download specific document. Owner will send encrypted secret key and session key to client to decrypt the document.

Algorithm:
AES Encryption Process:

KeyGenCE(M) → K is the key generation algorithm that maps a data copy M to a convergent key K;

EncCE(K,M) → C is the encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs cipher text C;

DecCE(K,C) → M is the decryption algorithm that takes both the cipher text C and the convergent key K as inputs and then outputs the original data copy M;

TagGen (M) → T(M) is the tag generation algorithm that maps the original data copy M and outputs a tag T(M).

IV. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

V. CONCLUSION

Our propose technique provides data security using data encryption in cloud environment. We introduce a relative addressing method in which data will check at entry level when user uploading phases. Data privacy has become extremely important in the Cloud environment. The object interface offers storage that is secure and easy to share across platforms.

REFERENCES

[1] Mashayekhy, An Online Mechanism for Resource Allocation and Pricing in Clouds, IEEE Transactions on Computers, 12 June 2015.

[2] Himani, Cost-Deadline Based Task Scheduling in Cloud Computing, Advances in Computing and Communication Engineering (ICACCE), 1-2 May 2015.

[3] Aazam, Cloud Customer's Historical Record Based Resource Pricing, IEEE Transactions on Parallel and Distributed Systems , 27 August 2015.

[4] Abbadi, Towards Trustworthy Resource Scheduling in Clouds, IEEE Transactions on Information Forensics and Security, 25 February 2013.

[5] Feng, Price Competition in an Oligopoly Market with Multiple IaaS Cloud Providers, IEEE Transactions on Computers, 31 July 2013.

[6] Toosi, Revenue Maximization with Optimal Capacity Control in Infrastructure as a Service Cloud Markets, IEEE Transactions on Cloud Computing, 18 December 2014.

[7] Li, Negotiation-based resource provisioning and task scheduling algorithm for cloud systems, Quality Electronic Design (ISQED), 15-16 March 2016.